FORMAL STATEMENT

J. William Leonard
Director, Information Security Oversight Office
National Archives and Records Administration

before the

Committee on Government Reform
Subcommittee on National Security, Emerging Threats,
and International Relations
U.S. House of Representatives

August 24, 2004

Chairman Shays, Mr. Kucinich, and members of the Subcommittee, I wish to thank you for holding this hearing on security classification and declassification issues as well as for inviting me to testify today. As Director of the Information Security Oversight Office (ISOO), I am responsible to the President for overseeing the Government-wide security classification program in both Government and industry. An administrative component of the National Archives and Records Administration, my office receives policy and program guidance from the National Security Council. Our authority is found in two Executive orders, Executive Order 12958, as amended, "Classified National Security Information," and Executive Order 12829, as amended, "National Industrial Security Program."

It is Executive Order 12958 that sets forth the basic framework by which executive branch agencies classify national security information. Pursuant to his constitutional authority, in this Order the President authorizes a limited number of officials to apply classification to certain national security related information. While the Order is clear that the employment of classification is an inherently discretionary act, based in large part upon the judgment of an original classifying authority, in delegating classification authority the President has established clear parameters for its use and certain burdens that must be satisfied. Specifically, every act of classifying information must be able to trace its origin to an explicit decision by a responsible official who has been expressly delegated original classification authority. In addition, when required, the original classification authority must be able to identify or describe the damage to national security that would arise if the information were subject to unauthorized disclosure. Furthermore, the information must be owned by, produced by or for, or under the control of the United States Government; and finally, it must fall into one or more of the categories of information specifically provided for in the Order.[1]

It is important to recognize that classification authority is not without limits. The President has spelled out some very clear prohibitions with respect to the use of

---

[1] Pursuant to § 1.4 of the Order, information shall not be considered for classification unless it concerns: (a) military plans, weapons systems, or operations; (b) foreign government information; (c) intelligence activities (including special activities), intelligence sources or methods, or cryptology; (d) foreign relations or foreign activities of the United States, including confidential sources; (e) scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism; (f) United States Government programs for safeguarding nuclear materials or facilities; (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or (h) weapons of mass destruction.

classification. Specifically, in no case can information be classified in order to conceal violations of law or to prevent embarrassment to a person, organization or agency. Unfortunately, there have been instances giving the impression that information has been classified in violation of the Order. In each case I am aware of, I do not believe it arose out of mal intent on the part of any individual. Rather, it often arises due to a lack of proactive oversight within agencies and a lack of effective training and awareness provided to some cleared personnel. In every instance that comes to our attention, we work with the agencies involved in order to ensure that adequate corrective action is taken.

I believe that the overall policy for security classification as set forth in the current Executive order is fundamentally sound. While I and others, to include the "9/11 Commission," have advocated revisions to basic concepts such as the "need-to-know" principle, the Order as currently configured is replete with measures to ensure the classification system's continued effectiveness. For example, each agency must appoint a senior official to oversee its program, promulgate internal regulations, establish and maintain security education and training programs, as well as an ongoing self-inspection program, and commit the resources necessary to ensure effective implementation of the program. Many agencies are excelling at fulfilling these requirements; others are not.

For example, it is no secret that the Government classifies too much information. In my over 30 years of experience in security and counterintelligence matters, I have observed that many senior officials will candidly acknowledge the problem of excessive classification, although oftentimes the observation is made with respect to the activities of agencies other than their own. The potential issue of excessive classification is supported, in part, by agency input to my office that indicates that overall classification activity is up over the past several years. For example, based upon information furnished our office, the total number of classification decisions increased from 9 million in FY 2001 to 11 million in FY 2002 and 14 million in FY 2003. However, these increases do not necessarily indicate a penchant for secrecy on the part of Federal agencies — they also reflect how busy these agencies are. Since 9/11, and especially with respect to the Global War on Terrorism and the Iraq War, more and more agency operations have been working on a 24/7 basis — which will naturally increase the activities' overall output, to include the number of classification decisions.

That said, I believe a more meaningful metric is the number of original classification decisions made within agencies (i.e., the initial determination by an authorized classifier that specific information requires protection in the interest of national security). Those reported figures are up 8 percent over the number of original classification decisions reported in FY 2002.

What I find most troubling, however, is that some individual agencies have no real idea how much information they generate is classified; whether the overall quantity is increasing or decreasing; what the explanations are for such changes; which elements within their organizations are most responsible for the changes; and most importantly of all whether the changes are appropriate (i.e., whether too much or too little information is being classified and whether for too long or too short a period of time). The identification of baseline information such as this would help agencies ascertain the effectiveness of their classification efforts.

My current concerns extend to the area of declassification as well. One of the principal procedures for maintaining the effectiveness of the classification system is the purging from the safeguarding system of information that no longer requires protection in the interest of national security. In addition to processes such as automatic and systematic declassification, as well as mandatory declassification reviews, the Executive Order clearly states that "information shall be declassified as soon as it no longer meets the standards for classification" (§ 3.1). Elsewhere, the Order specifically prohibits the use of classification "to prevent or delay the release of information that does not require protection in the interest of the national security" (§ 1.7 (a) (4)). Declassification cannot be regarded as a "fair weather project," something we tend to when resources are plentiful but which quickly falls off the priority list when times get tough, especially in times of national security challenges. Nonetheless, it is disappointing to note that declassification activity has been down for the past several years.

In some quarters, when it comes to classification in times of national security challenges, when available resources are distracted elsewhere, the approach toward classification can be to "err on the side of caution," by classifying and delaying declassification "when in doubt" and "asking questions later." Yet, the classification system is too important, and the consequences resulting from improper implementation too severe, to allow "error" to be a part of any implementation strategy. Error from either perspective, both too little and too much classification, is not an option. Too much classification unnecessarily impedes effective information sharing, and inappropriate classification undermines the integrity of the entire process. Too little classification can subject our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations to potential harm. It is in this regard that proactive oversight by an agency of its security classification program is crucial. To allow information that will not cause damage to national security to remain in the classification system, or to enter the system in the first instance, places all classified information at needless increased risk.

In response to these concerns, I have recently written to all agency heads asking them to closely examine their efforts in addressing the basics in establishing and maintaining an effective security classification program at their agency. All have been asked to give special emphasis to reviewing how they provide their personnel who deal with classified information the knowledge and understanding required to make the program work, and what positive steps they take to ensure the continued integrity of the system. This

includes ensuring that information that requires protection is properly identified and safeguarded; and, equally important, that information not eligible for inclusion in the classification system remains unclassified or is promptly declassified.

It is essential to recognize that the security classification system is permissive, not prescriptive — it identifies what information can be classified, not what information must be classified. The decision to classify information or not is ultimately the prerogative of an agency and its original classification authorities. The problem, however, is, with all due apologies to John Donne, no agency is an island. The exercise of agency prerogative to classify certain information has ripple effects throughout the entire executive branch. For example, it can serve as an impediment to sharing information with another agency, or with the public, who have a genuine need-to-know for the information. In addition, under some circumstances, it can actually undermine individuals' confidence in the integrity of the overall system, to include cleared individuals, an outcome with serious implications for everyone.

The 9/11 Commission has recommended that "Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge". The Administration is currently developing guidelines and regulations to improve information-sharing both among Federal Departments and Agencies and between the Federal Government and state and local entities. On August 2, 2004, President Bush announced that he will be issuing a directive requiring all relevant

agencies to complete the task of adopting common databases and procedures so that intelligence and homeland security information can be shared and searched effectively, consistent with privacy and civil liberties.

I commend the President's leadership in this area, and my office, working through the appropriate agencies, will be examining and advising on issues relating to the "need-to-know" and the "third-agency rule," as set forth in E.O. 12958, as amended. The current framework governing the safeguarding of classified information is based upon the "push" model of information management. The need-to-know principle and the third-agency rule give the authorized holder of the information the sole prerogative of determining whether a prospective recipient requires access to specific information (see § 4.1 (c) of the Order). The Executive Order goes on to state that classified information originated in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency (§ 4.1 (i)). These principles reflect the premise that national security considerations always necessitate the restriction of the dissemination of classified information and that originators of classified information are omniscient and are cognizant of all possible uses of the information. As pointed out by the "9/11 Commission," the reality is that national security can be placed at risk if classified information is not effectively shared.

In the final analysis, it is the people who deal with the information, their knowledge and understanding of the program, their faith in the integrity of the system represented by the classification markings, and their belief that everyone in the executive branch will do

what is expected of them that protects truly sensitive information from unauthorized disclosure. This knowledge, understanding, confidence, and expectation cannot be taken for granted. The integrity of the system will not be maintained on its own. It requires clear, forceful and continuous effort by senior leadership to make it happen. And the integrity of the security classification program is essential to our nation's continued well-being. The consequences of failure are too high. Thus, the American people expect and deserve nothing less than that we get it right each and every day.

Again, I thank you for inviting me here today, Mr. Chairman, and I would be happy to answer any questions that you or the Subcommittee might have.